Kürzungsregel für Kongruenzen

Erinnere dich an die folgende Rechenregel für Kongruenzen:

$$\boldsymbol{a \cdot c \equiv b \cdot c \mod m \iff a \equiv b \mod \frac{m}{\mathrm{ggT}(c,m)}}$$

Eine Erklärung für die Rechenregel findest du am Arbeitsblatt – Kongruenz und Restklassen.

Wenn c und m teilerfremd sind, dann gilt also:

$$a \cdot c \equiv b \cdot c \mod m \iff a \equiv b \mod \_\_\_\_$$

Kleiner Satz von Fermat (1640)

Für jede ganze Zahl a und jede Primzahl p gilt der **Kleine Satz von Fermat**:

$$\boldsymbol{a^p \equiv a \mod p}$$

Zum Beispiel: $\underbrace{4^5}_{=1024} \equiv 4 \mod 5$

Wenn a kein Vielfaches von p ist, dann gilt $\mathrm{ggT}(a,p) = \_\_\_\_$ und damit:

$$\boldsymbol{a^{p-1} \equiv 1 \mod p}$$

Pascalsches Dreieck & Primzahlen

p ist eine Primzahl. Rechts siehst du die obersten 12 Reihen vom Pascalschen Dreieck:

In jeder „Primzahlreihe“ sind alle Zahlen im Inneren jeweils Vielfache dieser Primzahl.

Zum Beispiel: Die Zahlen

7, 21, 35, 35, 27, 7

sind alle durch 7 teilbar.

Das ist kein Zufall.

					1						
				1		1					
$p=2$			1		2		1				
$p=3$		1		3		3		1			
			1		4		6		4		1
$p=5$		1		5		10		10		5		1
	1		6		15		20		15		6		1
$p=7$	1		7		21		35		35		21		7		1
	1		8		28		56		70		56		28		8		1
	1		9		36		84		126		126		84		36		9		1
	1		10		45		120		210		252		210		120		45		10		1
$p=11$	1		11		55		165		330		462		462		330		165		55		11		1

Die Zahlen in Reihe p sind die folgenden Binomialkoeffizienten:

$$\binom{p}{0}, \binom{p}{1}, \binom{p}{2}, \binom{p}{3}, \dots, \binom{p}{p-1}, \binom{p}{p} \quad \text{mit} \quad \binom{p}{k} = \frac{\overbrace{p \cdot (p-1) \cdot (p-2) \cdot \ldots \cdot (p-k+1)}^{k \text{ Faktoren}}}{k!}$$

Erkläre, warum die Primzahl p den Binomialkoeffizienten $\binom{p}{k}$ für alle k mit $1 \le k \le p-1$ teilt.

Kleiner Satz von Fermat – Beweis ($a \geq 0$)

Wir beweisen jetzt $\boldsymbol{a^p \equiv a \mod p}$ für alle Primzahlen p mit vollständiger Induktion nach $a \geq 0$.
Dabei verwenden wir die beiden folgenden Aussagen:

- Binomischer Lehrsatz: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k}$
- $\binom{p}{k} \equiv 0 \mod p$ für alle Primzahlen p und $1 \leq k \leq p-1$.

1) Überprüfe den **Induktionsanfang** für $a = 0$:

2) Überprüfe den **Induktionsschritt** $a \to a+1$:
Du darfst also verwenden, dass $a^p \equiv a \mod p$ gilt.
Daraus musst du folgern, dass auch $(a+1)^p \equiv a+1 \mod p$ gilt.

□

Kleiner Satz von Fermat – Beweis ($a < 0$)

1) Für die gerade Primzahl $p = 2$ können wir $\boldsymbol{a^2 \equiv a \mod 2}$ für alle ganzen Zahlen a direkt beweisen:

- Wenn a gerade ist, dann ist a^2 eine gerade / ungerade Zahl.
- Wenn a ungerade ist, dann ist a^2 eine gerade / ungerade Zahl.

Streiche jeweils durch.

Die ganzen Zahlen a und a^2 liegen also in der gleichen Restklasse modulo 2.

2) Für jede ungerade Primzahl p und *negative* ganze Zahl a haben wir $(-a)^p \equiv (-a) \mod p$ gezeigt.
Folgere daraus, dass auch $a^p \equiv a \mod p$ gilt.

Also gilt $a^p \equiv a \mod p$ auch für alle negativen ganzen Zahlen a.

Leonhard Euler (1707-1783) bewies, dass eine Verallgemeinerung von $a^{p-1} \equiv 1 \mod p$ nicht nur für Primzahlen p stimmt, sondern für beliebige natürliche Zahlen.
Als Nächstes sehen wir uns diesen **Satz von Euler** und einen eleganten Beweis dafür an.
Der Satz von Euler spielt eine wichtige Rolle in der modernen Verschlüsselung.

Mehr dazu erfährst du am Arbeitsblatt – RSA-Verfahren.

Eulersche Phi-Funktion

Die **Eulersche Phi-Funktion** φ ist für jede natürliche Zahl $n \geq 1$ definiert.
$\varphi(n)$ ist die Anzahl natürlicher Zahlen a, für die $1 \leq a \leq n$ und $\text{ggT}(a, n) = 1$ gilt. Kurz:

$$\boldsymbol{\varphi(n) = |\{a \in \mathbb{N} \mid 1 \leq a \leq n \wedge \text{ggT}(a, n) = 1\}|}$$

Eulersche Phi-Funktion

Ermittle die folgenden Funktionswerte der Eulerschen Phi-Funktion.

1) $\varphi(1) =$ _____ **4)** $\varphi(4) =$ _____ **7)** $\varphi(7) =$ _____ **10)** $\varphi(10) =$ _____

2) $\varphi(2) =$ _____ **5)** $\varphi(5) =$ _____ **8)** $\varphi(8) =$ _____ **11)** $\varphi(11) =$ _____

3) $\varphi(3) =$ _____ **6)** $\varphi(6) =$ _____ **9)** $\varphi(9) =$ _____ **12)** $\varphi(12) =$ _____

Eulersche Phi-Funktion

p und q sind verschiedene Primzahlen.

1) Für welche natürlichen Zahlen a mit $1 \leq a \leq p$ gilt $\text{ggT}(a, p) = 1$?

_____ $\Longrightarrow$ $\varphi(p) =$ _____

2) Für welche natürlichen Zahlen a mit $1 \leq a \leq p^k$ gilt *nicht* $\text{ggT}(a, p^k) = 1$?

_____ $\Longrightarrow$ $\varphi(p^k) =$ _____

3) Für welche natürlichen Zahlen a mit $1 \leq a \leq p \cdot q$ gilt *nicht* $\text{ggT}(a, p \cdot q) = 1$?

$\Longrightarrow$ $\varphi(p \cdot q) =$ _____ $= \varphi(p) \cdot \varphi(q)$

Multiplikativität der Eulerschen Phi-Funktion

Tatsächlich ist die Eulersche Phi-Funktion für alle *teilerfremden* Zahlen m und n multiplikativ.

Aus $\text{ggT}(m, n) = 1$ folgt also $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Primfaktorzerlegung von $n \rightsquigarrow \varphi(n)$

Zerlege n in Primfaktoren und berechne $\varphi(n)$.

a) $n = 42$ **b)** $n = 360$

Satz von Euler (1736)

Wenn $\text{ggT}(a,n)=1$ ist, dann gilt der **Satz von Euler**:

$$\boldsymbol{a^{\varphi(n)} \equiv 1 \mod n}$$

Wenn n eine Primzahl ist, dann ist das der Satz von Fermat.

mod 100

Ermittle mit dem Satz von Euler die letzten beiden Dezimalstellen von 23^{42}.

Kongruenz & ggT

Für den Beweis vom Satz von Euler verwenden wir zwei Eigenschaften:

1) $\boldsymbol{a \equiv b \mod n \implies \text{ggT}(a,n) = \text{ggT}(b,n)}$

Alle Zahlen, die in der gleichen Restklasse modulo n sind, haben mit n den gleichen größten gemeinsamen Teiler.

Begründe die Aussage:

Hinweis: $\text{ggT}(a+k\cdot n, n) = \text{ggT}(a,n)$

2) Wenn $\text{ggT}(a,n)=1$, dann gilt: $\boldsymbol{x\cdot a \equiv y\cdot a \mod n \iff x \equiv y \mod n}$

Satz von Euler – Beweis

Damit beweisen wir jetzt $\boldsymbol{a^{\varphi(n)} \equiv 1 \mod n}$ für alle Zahlen a mit $\text{ggT}(a,n)=1$.

Unter den Zahlen $\{1,2,3,\ldots,n\}$ gibt es $\varphi(n)$ verschiedene Zahlen, die zu n teilerfremd sind.
Wir geben diesen $\varphi(n)$ verschiedenen Zahlen jeweils einen Namen: $\{a_1, a_2, a_3, \ldots, a_{\varphi(n)}\}$

Aus $\text{ggT}(a_i,n)=1$ und $\text{ggT}(a,n)=1$ folgt $\text{ggT}(a_i\cdot a, n) =$ _____ .

Wegen **1)** muss $a_i\cdot a$ in der gleichen Restklasse modulo n wie eine der Zahlen $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ sein.
Wegen **2)** sind die Zahlen $a_1\cdot a$, $a_2\cdot a$, … , $a_{\varphi(n)}\cdot a$ alle in verschiedenen Restklassen modulo n, denn:

$$a_i\cdot a \equiv a_j\cdot a \mod n \overset{2)}{\implies} a_i \equiv a_j \mod n \implies a_i = a_j$$

„Indirekter Beweis“

Die Multiplikation mit a vertauscht also nur die Reihenfolge der $\varphi(n)$ verschiedenen Restklassen.

$$\implies a_1\cdot a_2\cdot\ldots\cdot a_{\varphi(n)} \equiv (a_1\cdot a)\cdot(a_2\cdot a)\cdot\ldots\cdot(a_{\varphi(n)}\cdot a) \mod n$$
$$\implies a_1\cdot a_2\cdot\ldots\cdot a_{\varphi(n)} \equiv a_1\cdot a_2\cdot\ldots\cdot a_{\varphi(n)}\cdot a^{\varphi(n)} \mod n$$
$$\overset{2)}{\implies} 1 \equiv a^{\varphi(n)} \mod n$$

□